MEMORANDUM FOR HEADS OF SERVICES AND STAFF OFFICES AND
REGIONAL ADMINISTRATORS

FROM: MICHAEL W. CARLETON
CHIEF INFORMATION OFFICER (I)

SUBJECT: CIO Instructional Letter 06-02 - Safeguarding Personally Identifiable Information (PII)

This memorandum transmits the GSA Instructional Letter 06-02 - Safeguarding Personally Identifiable Information (PII)

The purpose of this Instructional Letter is to:

1. Provide additional direction and guidance in protecting personally identifiable information (PII) on GSA IT systems and any associated record of that information and
2. Adhere to OMB memoranda M-06-15 and M-06-16 issued to Heads of Departments and Agencies dealing with safeguarding and protecting PII and sensitive agency information.

This Instructional Letter has been vetted with all current Information Technology Council members and their comments have been reviewed and incorporated. We appreciate your continued cooperation in assisting to implement information technology improvements and security standardization to provide more efficient IT capability for all GSA associates.

Should you have any questions regarding this matter, contact me on (202) 501-1000, or Phil Klokis, Director, Office of Enterprise Investment Portfolio and Policy on (202) 501-3535.

Attachment

GENERAL SERVICES ADMINISTRATION
OFFICE OF THE CHIEF INFORMATION OFFICER
OFFICE OF THE CHIEF PEOPLE OFFICER

CIO IL-06-02
August 8, 2006

GSA Instructional Letter

SUBJECT: Safeguarding Personally Identifiable Information

1. Purpose. This Instructional Letter provides additional policy and direction about protecting personally identifiable information (PII) in GSA information technology (IT) systems and any associated record of that information, such as printed paper documents or other storage media. PII is any personal information that is associated with a unique identifier and can be accessed through that identifier. A personal identifier usually is a name plus another piece of information such as a Social Security Number (SSN), but can be any designation that is unique to a particular person. Personal information, for Federal government purposes, is any information that is protected by the Privacy Act. This includes personal information collected about public individuals. It also includes information collected about Federal personnel, with some exceptions for work-related information. In addition to name and SSN, some PII examples are a name plus home street and e-mail addresses, home and emergency telephone numbers, date of birth, marital status, race, sex, national origin, qualifications, medical history, private sector employment history, financial and credit records, grievances and appeals, legal and arrest records, and information about some (but not all) personnel actions.

2. Background. Title III of the E- Government Act of 2002, also known as the Federal Information Security Management Act (FISMA), states that the agency Chief Information Officer is responsible for training and overseeing personnel with information security responsibilities, and for ensuring that agency personnel comply with FISMA requirements. Additionally, the Agency Senior Official for Privacy is tasked by OMB with ensuring implementation of information privacy protections. This instructional letter addresses both information privacy and information security since the same access controls and system security technologies are essential to safeguarding personal and sensitive information.

OMB memoranda sent from Clay Johnson III, Deputy Director for Management, M-06-15, Safeguarding Personally Identifiable Information (issued May 22, 2006) and M-06-16, Protection of Sensitive Agency Information (issued June 23, 2006), provide the guidance for this Instructional Letter.

3. Clearance due date. Copies of this IL will be sent to all Clearance Officers with a five (5), working day lead time for responses. Responses will be reviewed and consideration given for inclusion if a decision is made to change this IL

into an order.

4. Expiration date. One year from the signing of this instructional letter or upon cancellation or incorporation into a subsequent order.

5. Applicability. This instructional letter applies to all GSA employees, other government agency employees, GSA contractors, and others who may access, use, or otherwise handle PII in the performance of their official duties. This instructional letter does NOT apply to individuals accessing their own PII from sources such as payroll or the CHRIS system.

6. Policy Statement. In addition to the security requirements outlined in GSA IT Security Policy (CIO P 2100.1C) and the GSA Privacy Act Program (CPO 1878.1), the following security requirements apply to the protection of PII.

a. An employee shall not remove PII from GSA facilities (including GSA managed programs housed at contractor facilities under contract), or accessed remotely (i.e., from locations other than GSA facilities), without written permission from the employee's supervisor, the data owner, and the IT system authorizing official. This applies to electronic media (e.g. laptops, Blackberries, USB drives), paper, and any other media (e.g., CDs/DVDs) that may contain PII.

b. For continuity of operations plan (COOP) contact lists which only contain a person's name and home phone number, the requirements in paragraph a. above and e. below do not apply. COOP contact lists kept on an electronic device that is password protected (Blackberry, handheld device, laptop, USB drive) do not require written permission or encryption. Paper "cascade lists" limited to name and home phone number that are maintained for the purpose of emergency employee accountability are permissible with the approval of those individuals listed. All paper and other media should be kept in a locked facility or an otherwise secure location when not in use.

c. PII shall not be stored on or accessed from personally owned computers or personally owned mobile devices. PII shall only be accessed from government furnished equipment (GFE) or contractor maintained computers configured in accordance with GSA IT security policy and technical security standards.

d. PII shall be stored on network drives and/or in application databases with proper access controls (i.e., user ID/password) and shall be made available only to those individuals with a valid need to know.

e. If it is a business requirement to store PII on GSA user workstations or mobile devices including, but not limited to notebook computers, USB drives, CD-ROMs/DVDs, personal digital assistants and Blackberries, PII must be encrypted using an approved National Institute of Standards and Technology (NIST) algorithm, i.e., Triple Data Encryption Standard (3DES) or Advanced Encryption Standard (AES). Certified encryption modules must be used to the greatest extent possible in accordance with FIPS PUB 140-2, Security Requirements for Cryptographic Modules.

f. Recommended methods of file encryption include:

1) WinZip 9.0, 256 bit AES encryption;
2) Microsoft encrypted file system (EFS), 256 bit AES encryption; and
3) Pretty Good Privacy (PGP), 256 bit AES encryption.

When using password generated encryption keys, a password of at least 8 characters with a combination of letters, numbers, and special characters is required. A password of at least 12 characters is recommended.

g. If PII needs to be transmitted over the Internet, it must be sent using encryption methods defined above (i.e., PGP, WinZip).

h. If PII needs to be emailed within the GSA network, at a minimum Lotus Notes encryption is required. For additional protection the information also can be encrypted as described above (i.e., PGP, WinZip).

i. All remote access connections and mobile devices shall automatically lock-out within 30 minutes of inactivity (15 minutes is already the requirement for computers and mobile devices).

j. Two factor authenticated remote access shall be fully implemented as part of the HSPD 12 Smart Card project within 2 years of the date of this instructional letter.

k. Creation of computer-readable data extracts that include PII shall be maintained in an official log including creator, date, type of information, and user.

l. All incidents involving personally identifiable information must be reported to the GSA OCIO Office of the Senior Agency Information Security Officer (OSAISO) within one hour of discovering the incident. GSA employees and contractors shall report to their Information Systems Security Officer (ISSO) and the OSAISO. If the ISSO cannot be reached the Information Systems Security Manager (ISSM) and OSAISO should be contacted. All incidents involving personally identifiable information in electronic or physical form must be reported. There should be no distinction between suspected and confirmed breaches. For ISSO, ISSM and OSAISO points of contact go to http://insite.gsa.gov/itsecurityprogram.

m. All authorizing officials for systems containing PII shall create and implement an identity theft prevention plan, including but not limited to putting a fraud alert on affected person's credit report, and providing one year of an identity theft monitoring service though one of the major consumer reporting agencies for any suspected or confirmed breaches of PII.

7. Compliance. Compliance with this instructional letter is mandatory. Failure to comply with this instructional letter may lead to disciplinary action and/or criminal penalties.

8. References. Contact your ISSO for further implementation guidance on the technical requirements in this instructional letter. The following informational material is relevant to this topic and should be consulted for additional background and guidance. Please go to the websites for further information.

a. GSA IT Security Policy (CIO P 2100.1C):
http://insite.gsa.gov/gsa/cm_attachments/INSITE_BASIC/securitypolicytransmittal_R21B42_0Z5RDZ-i34K-pR.pdf

b. GSA Privacy Act Program (CPO 1878.1):
http://insite.gsa.gov/gsa/cm_attachments/INSITE_BASIC/GSAOrder_R21B42_0Z5RDZ-i34K-pR.htm

Michael W. Carleton
CHIEF INFORMATION OFFICER

Gail T. Lovelace
CHIEF PEOPLE OFFICER